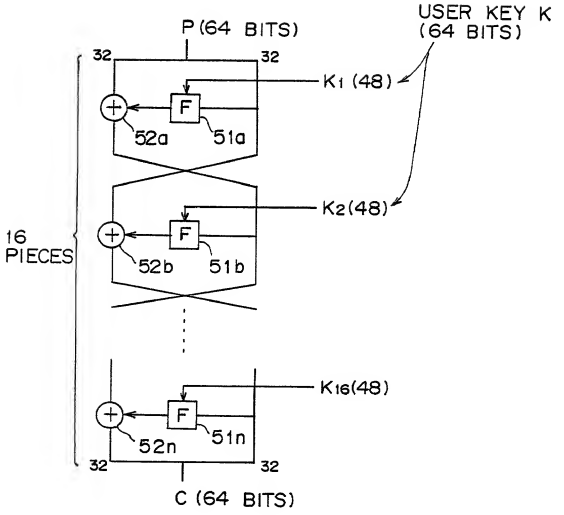

P (64 BITS)
USER KEY K
(64 BITS)
32
32
K1 (48)
F
52a
51a
K2(48)
16
PIECES
52b
51b
K16(48)
51n
52n
32
32
C (64 BITS)

FIG. 1A

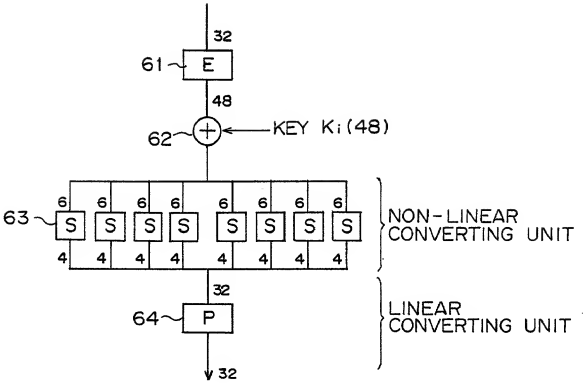


FIG. 1B

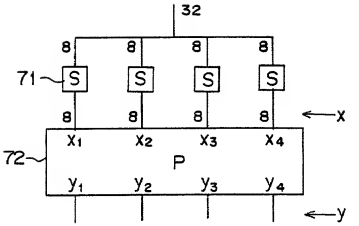


FIG. 1C

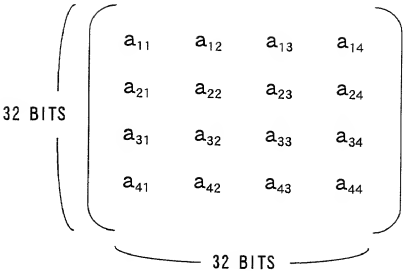

32 BITS
a_{11} a_{12} a_{13} a_{14}
a_{21} a_{22} a_{23} a_{24}
a_{31} a_{32} a_{33} a_{34}
a_{41} a_{42} a_{43} a_{44}
32 BITS

FIG. 1D

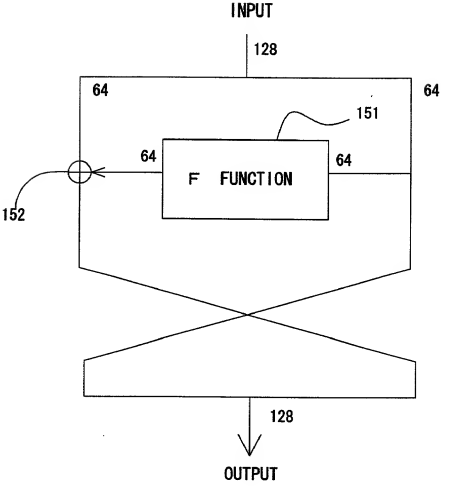
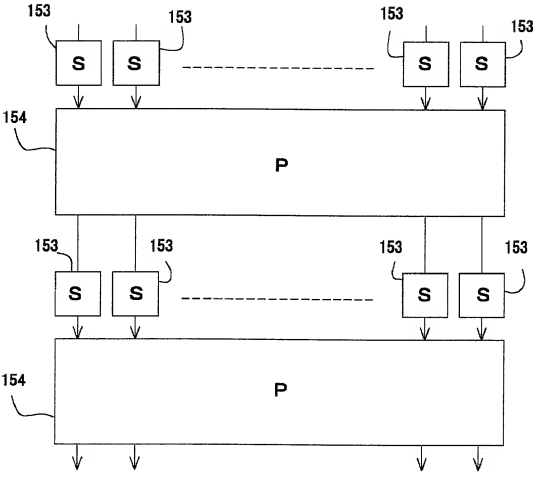


FIG. 1E



S : NON-LINEAR CONVERSION, P : LINEAR CONVERSION

FIG. 1F

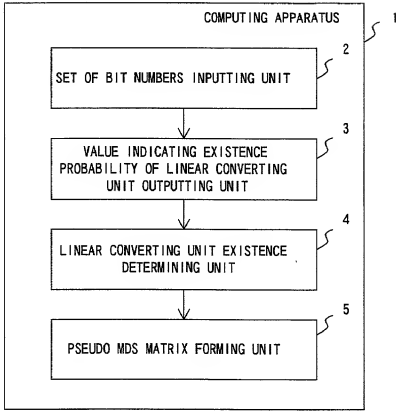


FIG. 2A

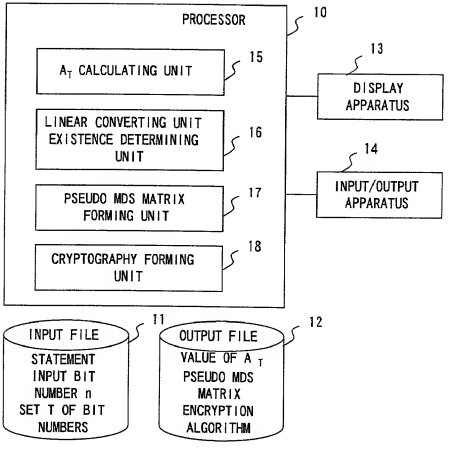

PROCESSOR
10
A_T CALCULATING UNIT
15
LINEAR CONVERTING UNIT EXISTENCE DETERMINING UNIT
16
PSEUDO MDS MATRIX FORMING UNIT
17
CRYPTOGRAPHY FORMING UNIT
18
13
DISPLAY APPARATUS
14
INPUT/OUTPUT APPARATUS
11
INPUT FILE
STATEMENT INPUT BIT NUMBER n SET T OF BIT NUMBERS
12
OUTPUT FILE
VALUE OF A_T PSEUDO MDS MATRIX ENCRYPTION ALGORITHM

FIG. 2B

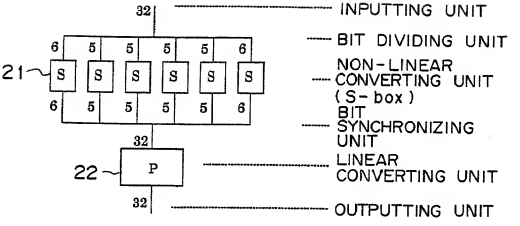


FIG. 3

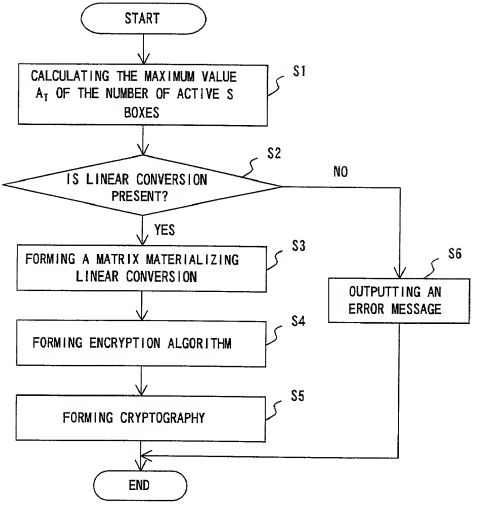

START
CALCULATING THE MAXIMUM VALUE A_T OF THE NUMBER OF ACTIVE S BOXES
S1
IS LINEAR CONVERSION PRESENT?
S2
NO
YES
FORMING A MATRIX MATERIALIZING LINEAR CONVERSION
S3
OUTPUTTING AN ERROR MESSAGE
S6
FORMING ENCRYPTION ALGORITHM
S4
FORMING CRYPTOGRAPHY
S5
END

FIG. 4

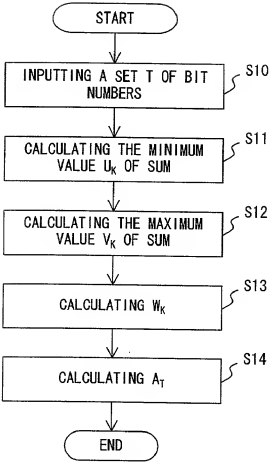

START
INPUTTING A SET T OF BIT NUMBERS
S10
CALCULATING THE MINIMUM VALUE U_K OF SUM
S11
CALCULATING THE MAXIMUM VALUE V_K OF SUM
S12
CALCULATING W_K
S13
CALCULATING A_T
S14
END

FIG. 5

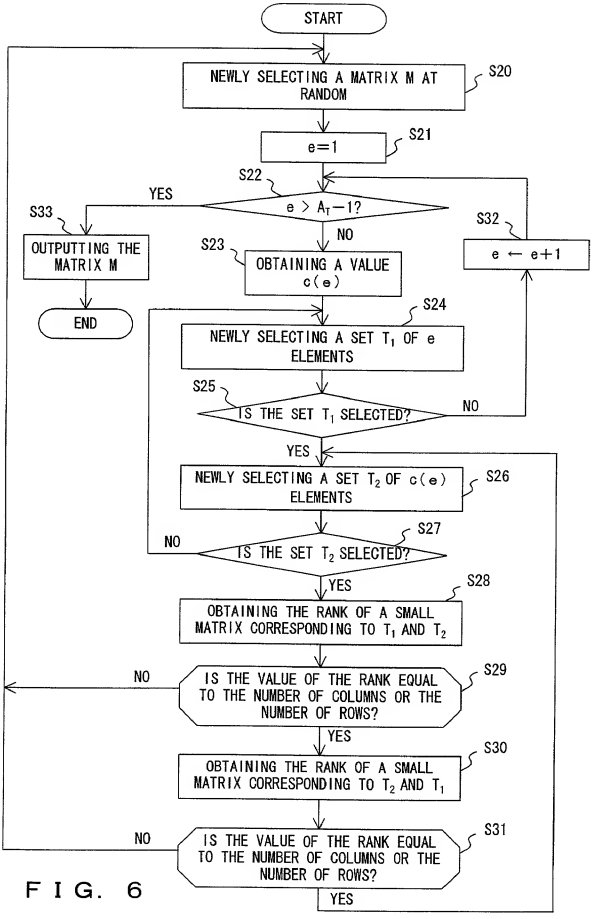


FIG. 6

$M =$

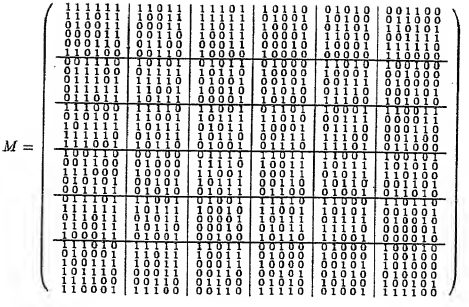


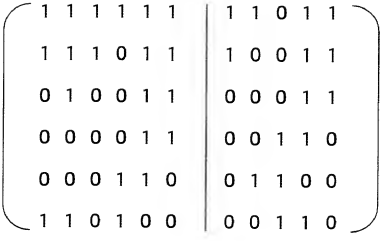
FIG. 7

$$M = \begin{array}{c} \begin{matrix} 6 & 5 & 5 & 5 & 5 & 6 \end{matrix} \\ \begin{pmatrix} M_{11} & M_{12} & M_{13} & M_{14} & M_{15} & M_{16} \\ M_{21} & M_{22} & M_{23} & M_{24} & M_{25} & M_{26} \\ M_{31} & M_{32} & M_{33} & M_{34} & M_{35} & M_{36} \\ M_{41} & M_{42} & M_{43} & M_{44} & M_{45} & M_{46} \\ M_{51} & M_{52} & M_{53} & M_{54} & M_{55} & M_{56} \\ M_{61} & M_{62} & M_{63} & M_{64} & M_{65} & M_{66} \end{pmatrix} \end{array} \begin{matrix} 6 \\ 5 \\ 5 \\ 5 \\ 5 \\ 6 \end{matrix} \Rightarrow \begin{pmatrix} M_{22} & M_{23} & M_{25} & M_{26} \\ M_{32} & M_{33} & M_{35} & M_{36} \\ M_{62} & M_{63} & M_{65} & M_{66} \end{pmatrix}$$

FIG. 8A

$$M = \begin{array}{c} \begin{matrix} 6 & 5 & 5 & 5 & 5 & 6 \end{matrix} \\ \begin{pmatrix} M_{11} & M_{12} & M_{13} & M_{14} & M_{15} & M_{16} \\ M_{21} & M_{22} & M_{23} & M_{24} & M_{25} & M_{26} \\ M_{31} & M_{32} & M_{33} & M_{34} & M_{35} & M_{36} \\ M_{41} & M_{42} & M_{43} & M_{44} & M_{45} & M_{46} \\ M_{51} & M_{52} & M_{53} & M_{54} & M_{55} & M_{56} \\ M_{61} & M_{62} & M_{63} & M_{64} & M_{65} & M_{66} \end{pmatrix} \end{array} \begin{matrix} 6 \\ 5 \\ 5 \\ 5 \\ 5 \\ 6 \end{matrix} \Rightarrow \begin{pmatrix} M_{22} & M_{23} & M_{26} \\ M_{32} & M_{33} & M_{36} \\ M_{52} & M_{53} & M_{56} \\ M_{62} & M_{63} & M_{66} \end{pmatrix}$$

FIG. 8B



$$\left(\begin{array}{cccccc|ccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

FIG. 9

$$
\left(\begin{array}{cccccc}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1
\end{array}\right)
$$

FIG. 10

```
0 : matrix[5,5]=
00000
00000
00000
00000
00000
0
1 : matrix[5,5]=
00001
00010
00100
01000
10000
1
2 : matrix[5,5]=
00010
00100
01000
10000
00101
1
3 : matrix[5,5]=
00011
00110
01100
11000
10101
1
4 : matrix[5,5]=
00100
01000
10000
00101
01010
1
5 : matrix[5,5]=
00101
01010
10100
01101
11010
1
6 : matrix[5,5]=
00110
01100
11000
10101
01111
1
7 : matrix[5,5]=
00111
01110
11100
11101
11111
1
8 : matrix[5,5]=
01000
10000
00101
01010
10100
1
9 : matrix[5,5]=
01001
10010
00001
00010
00100
1
10 : matrix[5,5]=
01010
10100
01101
11010
10001
1
11 : matrix[5,5]=
01011
10110
01001
10010
00001
1
12 : matrix[5,5]=
01100
11000
10101
01111
11110
1
13 : matrix[5,5]=
01101
11010
10001
00111
01110
1
14 : matrix[5,5]=
01110
11100
11101
11111
11011
1
15 : matrix[5,5]=
01111
11110
11001
10111
01011
1
```

FIG. 11

```
16 : matrix[5,5]=
10000
00101
01010
10100
01101
1
17 : matrix[5,5]=
10001
00111
01110
11100
11101
1
18 : matrix[5,5]=
10010
00001
00010
00100
01000
1
19 : matrix[5,5]=
10011
00011
00110
01100
11000
1
20 : matrix[5,5]=
10100
01101
11010
10001
00111
1
21 : matrix[5,5]=
10101
01111
11110
11001
10111
1
22 : matrix[5,5]=
10110
01001
10010
00001
00010
1
23 : matrix[5,5]=
10111
01011
10110
01001
10010
1
24 : matrix[5,5]=
11000
10101
01111
11110
11001
1
25 : matrix[5,5]=
11001
10111
01011
10110
01001
1
26 : matrix[5,5]=
11010
10001
00111
01110
11100
1
27 : matrix[5,5]=
11011
10011
00011
00110
01100
1
28 : matrix[5,5]=
11100
11101
11111
11011
10011
1
29 : matrix[5,5]=
11101
11111
11011
10011
00011
1
30 : matrix[5,5]=
11110
11001
10111
01011
10110
1
31 : matrix[5,5]=
11111
11011
10011
00011
00110
1
```

FIG. 12

$$\begin{pmatrix} 31 & 27 & 29 & 22 & 10 & 12 \\ 14 & 21 & 11 & 8 & 26 & 4 \\ 24 & 30 & 25 & 13 & 17 & 19 \\ 6 & 4 & 15 & 27 & 25 & 5 \\ 29 & 25 & 9 & 30 & 24 & 22 \\ 26 & 31 & 27 & 4 & 8 & 2 \end{pmatrix}$$

FIG. 13

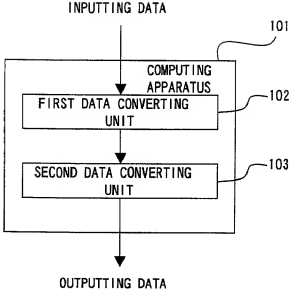


FIG. 14A

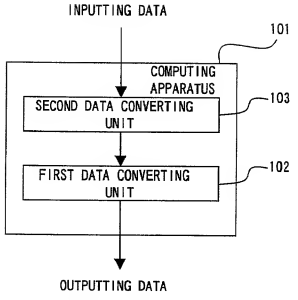


FIG. 14B

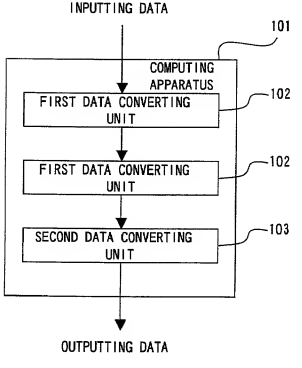


FIG. 14C

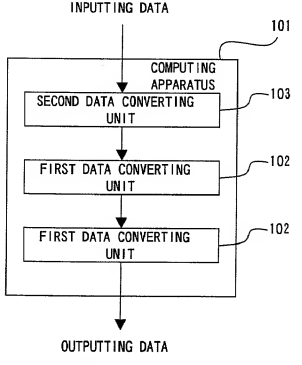


FIG. 14D

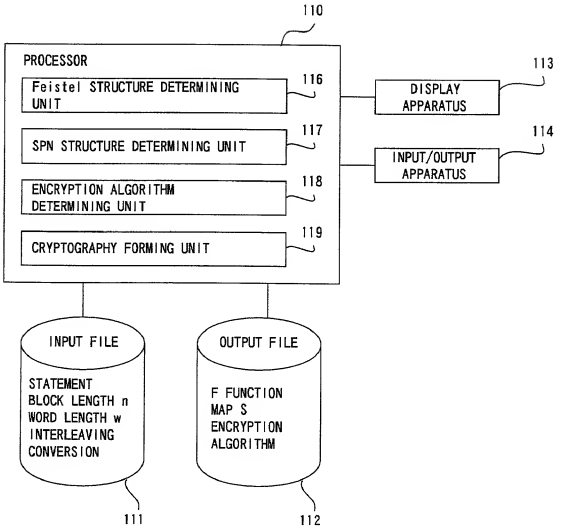

110
PROCESSOR
Feistel STRUCTURE DETERMINING UNIT
116
SPN STRUCTURE DETERMINING UNIT
117
ENCRYPTION ALGORITHM DETERMINING UNIT
118
CRYPTOGRAPHY FORMING UNIT
119
DISPLAY APPARATUS
113
INPUT/OUTPUT APPARATUS
114
INPUT FILE
STATEMENT
BLOCK LENGTH n
WORD LENGTH w
INTERLEAVING
CONVERSION
111
OUTPUT FILE
F FUNCTION
MAP S
ENCRYPTION
ALGORITHM
112

FIG. 15

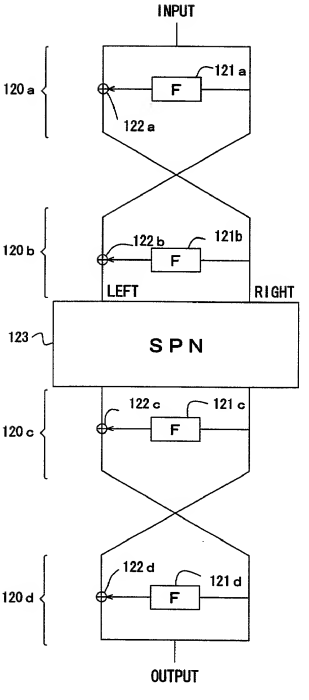
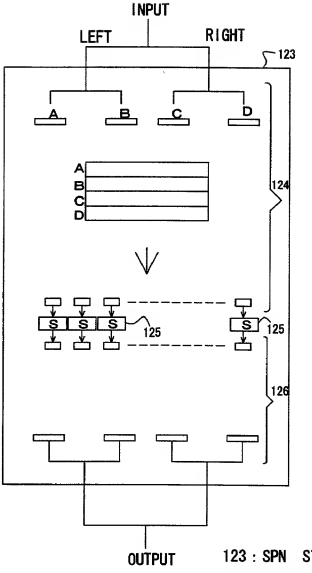

INPUT
120a
121a
F
122a
120b
122b
121b
F
LEFT
RIGHT
123
SPN
120c
122c
121c
F
120d
122d
121d
F
OUTPUT

FIG. 16



123 : SPN STRUCTURE
124 : INTERLEAVING CONVERSION
125 : S BOX
126 : INTERLEAVING REVERSE-CONVERSION

FIG. 17

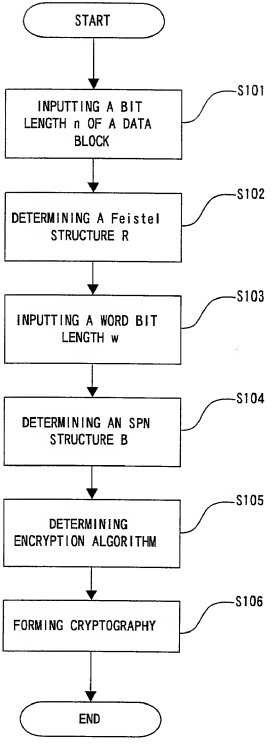

START
INPUTTING A BIT LENGTH n OF A DATA BLOCK
S101
DETERMINING A Feistel STRUCTURE R
S102
INPUTTING A WORD BIT LENGTH w
S103
DETERMINING AN SPN STRUCTURE B
S104
DETERMINING ENCRYPTION ALGORITHM
S105
FORMING CRYPTOGRAPHY
S106
END

FIG. 18

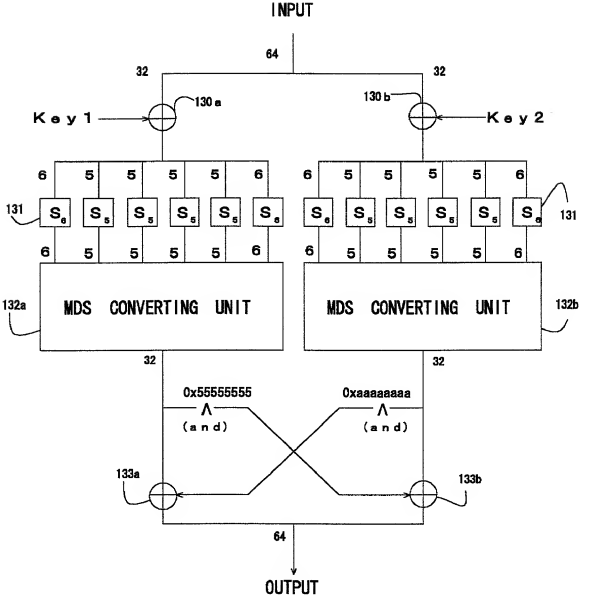

INPUT
64
32
32
Key 1
130a
130b
Key 2
6 5 5 5 5 6
6 5 5 5 5 6
131
131
S_6 S_5 S_5 S_5 S_5 S_6
S_6 S_5 S_5 S_5 S_5 S_6
6 5 5 5 5 6
6 5 5 5 5 6
132a
MDS CONVERTING UNIT
MDS CONVERTING UNIT
132b
32
32
0x55555555
0xaaaaaaaa
(and)
(and)
133a
133b
64
OUTPUT

FIG. 19

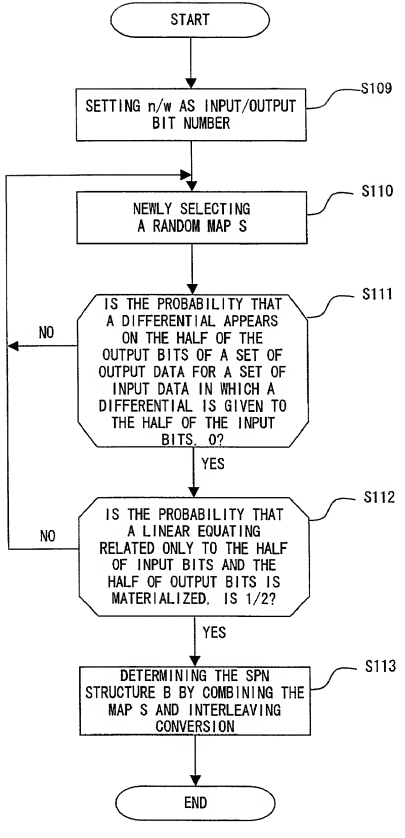

START
SETTING n/w AS INPUT/OUTPUT BIT NUMBER
S109
NEWLY SELECTING A RANDOM MAP S
S110
IS THE PROBABILITY THAT A DIFFERENTIAL APPEARS ON THE HALF OF THE OUTPUT BITS OF A SET OF OUTPUT DATA FOR A SET OF INPUT DATA IN WHICH A DIFFERENTIAL IS GIVEN TO THE HALF OF THE INPUT BITS, 0?
S111
NO
YES
IS THE PROBABILITY THAT A LINEAR EQUATING RELATED ONLY TO THE HALF OF INPUT BITS AND THE HALF OF OUTPUT BITS IS MATERIALIZED, IS 1/2?
S112
NO
YES
DETERMINING THE SPN STRUCTURE B BY COMBINING THE MAP S AND INTERLEAVING CONVERSION
S113
END

FIG. 20

INPUT DIFFERENTIAL	OUTPUT DIFFERENTIAL					
	(0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	2	2	0
(0010)	0	0	0	0	2	2
(0011)	0	0	0	2	0	2
(0100)	0	0	2	0	0	0
(1000)	2	0	4	0	0	0
(1100)	4	2	0	0	0	0

FIG. 21

INPUT BIT	OUTPUT BIT					
	(0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	-4	2	-2
(0010)	0	0	0	2	4	2
(0011)	0	0	0	-2	-2	0
(0100)	2	2	-4	0	0	0
(1000)	-2	-2	0	0	0	0
(1100)	0	4	0	0	0	0

FIG. 22

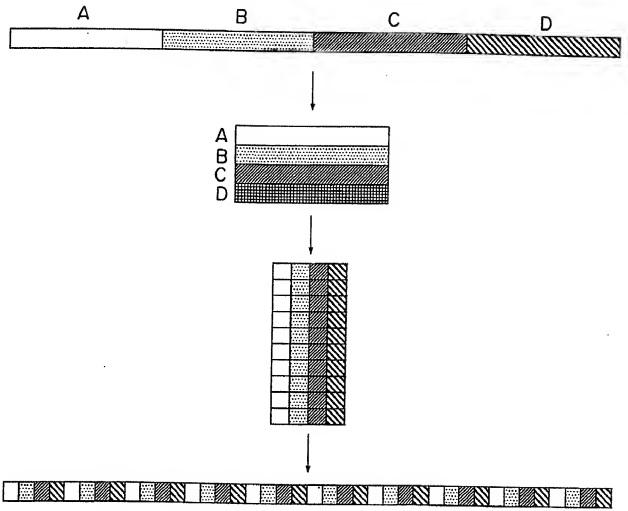


FIG. 23

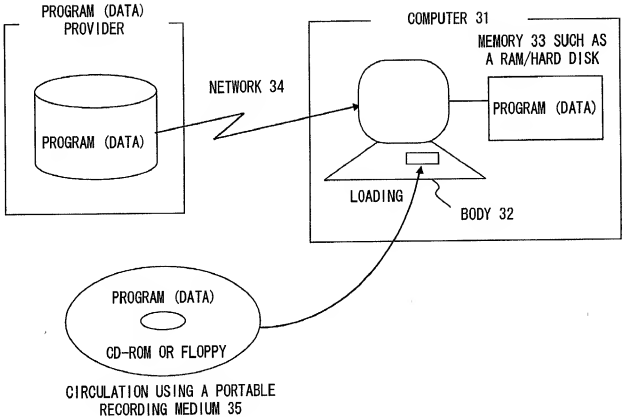


FIG. 24